8 6 AC

→ Network layer security : IPsec

* What is network layer Confidentiality

it means that between two network entities :

1. Sending entity encrypts datagram payload
   - payload Could be : TCP, UDP segment, ICMP or OSPF message.
2. all data sent from one entity to other would be hidden . data like :- web pages, email
3. blanket Coverage

---

* virtual private Networks (VPNs) :- Ⓐ

ك المؤسسات بتحتاج علشان تحافظ على خصوصياتها وشكلها
مشاكلها يعني يحتاجوا الحاجة ع الشبكات العادية من غير ما
تتوجه فحاجات من غيرها يضطروا يسوا شبكة خاصة

VPN : institution's inter-office traffic is sent over public internet instead. by :

1. encrypted before entering public internet
2. logically separate from other traffic

IPsec Services : → 1. data integrity
2. origin authentication
3. replay attack prevention
4. Confidentiality

protocols : 1. AH
2. ESP

unicef

-> IPsec datagram <-> emitted / received by end_systems
-> protects upper level protocols.

---

two IPsec protocols

Authentication Header (AH)	Encapsulation Security protocol (ESP)
-> provides:	-> provides:
① Source authentication	1 Source authentication
② data integrity	② data intergrity
* but no confidentiality	3 Confidentiality
	* widely used than AH

Four Combinations are possible

Host mode with AH	Host Mode with ESP	
Tunnel mode with AH	Tunnel Mode with ESP <-	most Common & Important

---

* Security associations (SAs)

إحنا قلنا ان الناس هتبعت الحاجة في الشبكة العامة اللي كل الناس
هتستخدمها بس هيعملوا traffic خاص بيهم وده انهم
هيبعتوا الداتا متشفرة من tunnels المفروض بين (SAs) دي
هي ال tunnels وبتبقى اتجاه واحد يعني لو A هيبعت لـ B
و B هيبعت لـ A كده انت محتاج 2 SAs والطرف التاني
معاه الحاجة اللي يقدر يفك بيها الشفرة بتاع ال Data ويقراها

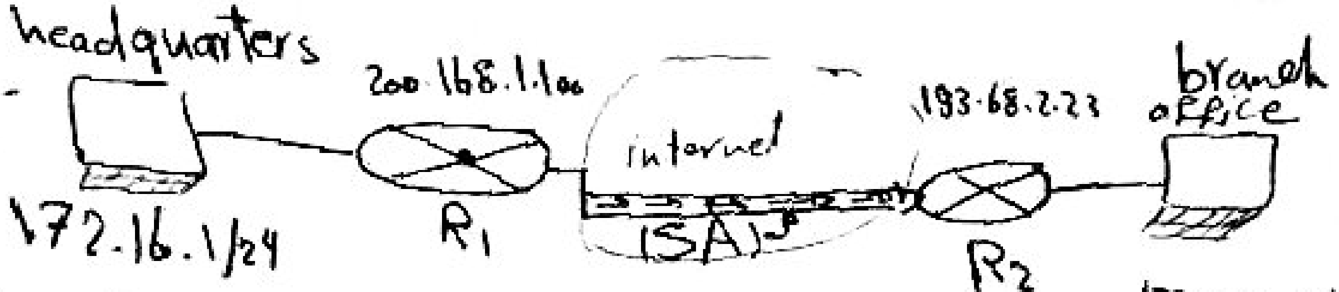
* before sending data SA is established from sending to receiving side
-> only one direction

يونيسف

* ending, receiving entitles maintain state information about SA
  - ↳ recall: TCP endpoints also maintain
  - ↳ state info.

IP is connectionless. IPsec is connection-oriented.

ex:


headquarters
200.168.1.100
internet
193.68.2.23
branch office
172.16.1/24
R1
(SA)
R2
172.16.2/24

وكده R1 هيفتح SA ل R2 ويبعت ماهو شاك R2 يفهم data

R1 stores for SA:-

1. 32-bit SA indentifier: security paramter index (SPI)
2. origin SA interface (200.168.1.100).
3. destination SA interface (193.68.2.23).
4. type of encryption used.
5. encryption key.
6. type of integrity check used.
7. authentication key.

unicef

* Security Association Database (SAD)

(4)

وده علشان ال endpoint لازم مكان يحتفظ فيه بال state بتاع ال SA اللى ماشيه دى

* endpoint holds SA state in SAD, to locate them during processing.

* with $\boxed{n}$ salespersons, $\boxed{2+2n}$ SAs in R1's SAD

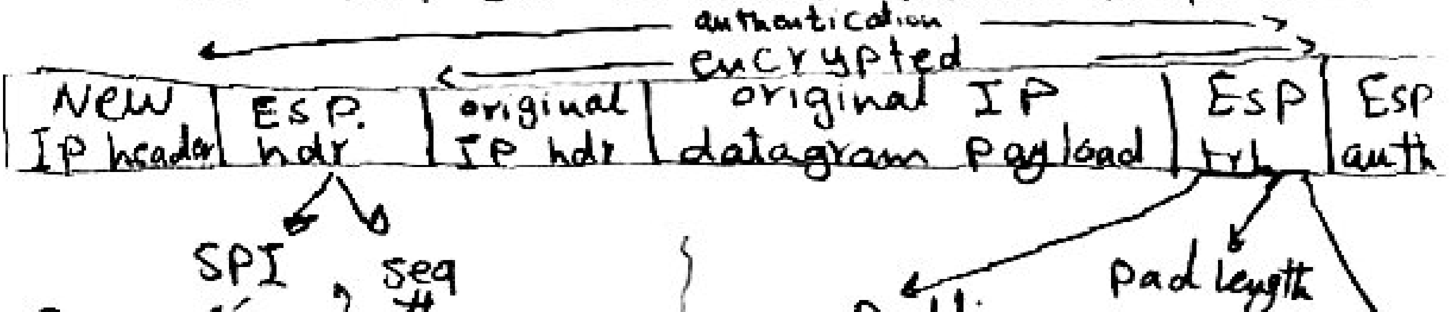
* When sending IPsec datagram, R1 access SAD to define process of datagram

* When ~~R2~~ IPsec datagram arrives to R2
  1. it examines SPI in IPsec datagram
  2. indexes SAD with SPI
  3. process datgram accordingly.

ص 93

HA
ESP → **IP sec datagram**

but this on tunnel mode with ESP.


authentication
encrypted
New IP header
ESP. hdr
original IP hdr
original IP datagram payload
ESP trl
ESP auth
SPI
seq #
Padding
pad length

SPI: so receiving side knows what to do.

seq #: to thwart replay attacks

attacks منع أى

ESP trailer: for block ciphers ← next header

الشفرة

R1: Convert original datagram to IPsec datagram

"والخمس الاوامر شرح ؟

* IPsec datagram

① appends to back of datagram an "ESP trailer" field.

② encrypts result using ①algorithm & ②key specified by SA

③ appends to front of encrypted quantity the ESP header

④ creates authentication MAC, using algorithm & key specified by SA

⑤ appends MAC to back of enchilada forming payload

⑥ creates brand new IP header with the classic IPV4 header fields, which it appends before payload.

unicef

(6)

* hints about Sequence numbers "Seq #"

→ for new SA, sender initialize seq # to 0

→ each time datagram is sent on SA

① Sender increments seq# count

② places value in seq# field

→ goal:

① prevent attackers from sniffing and replaying a packet

② receipt of duplicate, authenticated IP packets may disrupt service

→ method:

① destination checks for duplicates

② doesn't keep track of all received packets, but uses a window

---

Security policy Database (SPD)

rules [illegible]

"2 Databases"

① policy: for a given datagram, sending entity needs to know if it will use IP sec.

② it needs also to know wich SA to use

may use ⟷ source & des. IP address

may use ⟷ protocol number

③ info in SPD to know what to do?

④ " " SAD " " How " "?

7 IKE :- Internet Key Exchange

قبل كده كان ال endpoints تقعد تعمل IPsec
لو عدد ال users كتير تشغل ال manual مش هينفع
علشان كده عملوا الحاجة دة (IKE)

* manual keying is impractical for VPN with 100s of endpoints

* instead use (IPsec IKE)

IKE :- PSK & PKI

* authentication (prove who you are) with either
- ① pre-shared secret (PSK)
- ② PKI (public/private keys & certificates)

1 PSK :- both sides start with secret

* run IKE to authenticate each other and generate IPsec ([illegible]) including encryption, & Authentication key.

---

2 PKI :- both side start with public/private key pair.

1 run IKE to athenticate each other, obtain IPsec SAs ([illegible])

2 similar with handshake in SSL.

unicef
70 YEARS FOR EVERY CHILD

(8) IKE has two phases

phase 1 :- establish bi-directional IKE SA

* note IKE SA is differant from IPsec SA

phase 2 :- ISAKMP is used to securely negotiate IPsec pairs of SAs

(1) phase 1 has two modes

aggressive mode :-	(2) main mode :-
uses fewer messages	provides identity protection & more flexibil

يونيسف
٧٠ عام من اجل كل طفل

(8.7) Securing wireless LANs

p ١٠٤

وهنا الهدف ان يتم تأمين الـ wireless لأن ممكن يتم
إختراقه أكتر من الـ wired فهيحاولوا ان التصميم
تكون قريبه من الـ wired.

*WEP (wired equivalent privacy)

design goals:-

[1] symmetric key crypto:-
and this provides → confidentiality
→ data integrity
→ end-host authorization

[2] self-synchronizing:- each packet separately encrypted.

وده ان لو رسالة مثلا اتقسمت لأكتر من packet وتم تشفيرها
بالطريقة العادية كل packet هتعتمد ع الـ packet اللي اتبعتت قبلها
بس لو اللي قبلها ضاعت هي مش هتوصل برضه عشان كده هيفصلوا الـ
packets from each other.

[3] Efficient:-
implementable in hardware or software

unicef

(10) هنشرح كل نقطة من اللي فاتو

① Symmetric Stream Ciphers

وهنا بناخذ ال message وبنضيف عليها Key stream علشان تعملها encrypted

$m(i) \leftarrow$ unit of message

$Ks(i) \leftarrow$ " " Keystream

$C(i) \leftarrow$ encrypted message : $Ks(i) \overset{XOR}{\oplus} m(i)$

ولو عايز الرسالة بس "كده اكتشفها يعني"

$m(i) = Ks(i) \oplus C(i)$

والحاجة اللي بتعمل كدة فال WEP هي ال RC4

---

② فنقطة ال (Self synchronizing) علشان نحققها مش هياخذ قيمة ال key من ال packet السابقة، لا هيستخدم IV

↳ IV → initial value for every packet.

∴ packet (n+1) doesn't need to know where we left off for packet(n)

↳ WEP approach: initialize keystream with key + new IV for each packet

$$\text{key} + IV_{\text{packet}} \longrightarrow \boxed{\text{keystream generator}} \longrightarrow \text{keystream}_{\text{packet}}$$

يونيسف

(11) WEP encryption

(1) Sender Calculates ICV "Integrity Check Value" Over data

ودي عاملة يضمن ان الداتا اتوصل صح وسليمة

four-byte hash ← → CRC

---

(2) Sender creates (24-bit) IV, and appends it to key "gives 128-bit key"

---

(3) Sender append KeyID "8-bit field"

---

(4) 128-bit key inputted into random No. generator to get Keystream

---

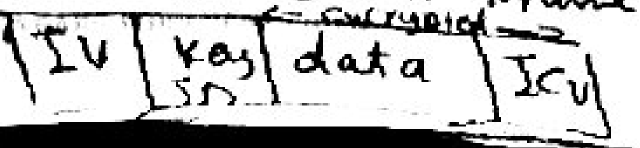
data+ICV

(5) keystream XoRed with data & ICV

data encrypted كده بقت

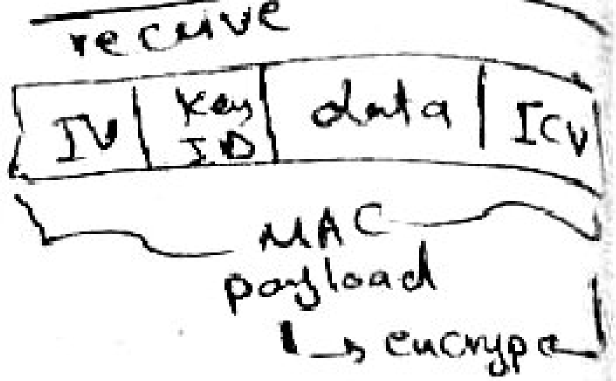
(2) IV + KeyID added to encrypted data and Create payload

(3) payload inserted in 802.11 frame



encrypted
IV
Key ID
data
ICV

WEP decryption



receive
IV
Key ID
data
ICV
MAC payload
encrypted

- receiver extract IV
- XoRs Keystream with encrypted data to decrypt it
- verifies data integrity with ICV

* WEP authentication:- [12]

sender → authentication request → router

← nonce (128 bytes)

nonce encrypted shared key →

← success if decrypted value = nonce

[illegible]

802.11
web encryption

* 24-bit IV, one IV per frame
  ∴ IV will eventually reused

802.11 → improved security

* stronger forms of encryption possible
* provides key distribution
* uses authentication server separate from access point. [illegible]

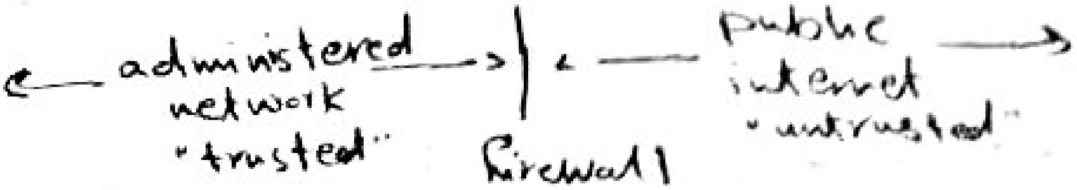
1130 EAP:- extensible authentication protocol. [illegible]

* end-end client to authentication server protocol
* EAP sent over separate links "wired"
  steps: [1] Mobile to AP
  [2] AP to authentication server

8.8 ١١٨ص (13)

operational security..
firewalls and IDS

* firewalls:..
isolates organization's internal net from larger internet, allowing some packets to pass, and block others


administered network "trusted"
firewall
public internet "untrusted"

* Why need firewalls:..

[1] prevent denial of service attacks
*SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real connections"

[2] prevent illegal modification/access of internal data

(3) allow only authorized access to inside network

---

types of firewalls:-

[1] stateless packet filters
(2) stateful " "
(3) application getaways

unicef
70 YEARS FOR EVERY CHILD

① stateless packet filters:- "heavy handed"

* internal network connected to internet via router firewall

* router filters packet by packet, decide to forward or drop the packet based on:-

1. source IP / destination IP "address"
2. TCP / UDP source & dest. port No.
3. ICMP message type
4. TCP SYN & ACK bits.

ص ١٠٠ + ص ١٠٢ سموا عليه

* ACL:- Access Control lists:-

table of rules, applied top to bottom to incoming packets (action, condition) pairs.

---

② stateful packet filtering:-

track status of every TCP connection

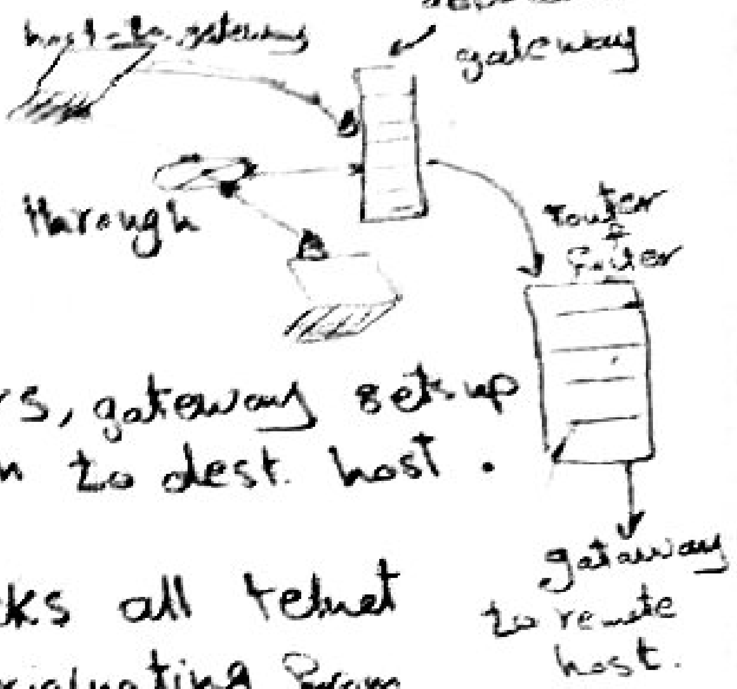
* track connection setup (SYN), teardown (FIN):- determine whether incoming & outgoing packet makes sense

* timeout inactive connections at firewall "no longer admit packets"

* ACL augmented to indicate need to check connection state table before admitting packet ص ١٠٥

3 Application gateways:

- Filter packets on app. data as well as on IP/TCP/UDP


host-to-gateway
application gateway
router & filter
gateway to remote host.

steps:-

1. require all telnet users to telnet through the gateway.

2. For authorized users, gateway setup telnet connection to dest. host.

3. router filter blocks all telnet connection not originating from gateway.

- limitations of firewalls & gateways

1. IP spoofing:- router can't know if data comes from claimed source

2. Filters often use all or nothing policy for UDP

3. trade off:- degree of communication with outside world, level of security

4. many highly protected sites still suffer from attacks.

5. Client software must know how to contact gateway.

unicef

اعرضنك :D

* Intrusion detection Systems. (IDS)

1 can do packet filtering..
→ operates on TCP/IP headers only.
→ no correlation check among sessions.

(2) IDS:.. A) deep palket inspection:.
→ Look at packet contents & check charalter string in palket that against database of known virus...

B) examine correlation among multiple packets
→ port scanning
→ Network mapping
→ D.o.s attalk